THE USAGE OF GRAPHICAL PASSWORD AS A REPLACEMENT TO THE ALPHANUMERICAL PASSWORD

Budi Hartanto, Bagus Santoso, Siauw Welly
Informatic Engineering, University of Surabaya
Jl. Raya Kalirungkut Surabaya – 60292
Email**:** budi@ubaya.ac.id

ABSTRACT: Alphanumerical password is the password scheme that obligates the users to enter characters as their password. In spite of its popularity, alphanumerical password usually can be cracked easily when it is used by novice users. Since these users usually type their password slowly, unauthorized person can get the password easily by observing the movement of the users' finger as they entering the password. A graphical password is proposed to replace the alphanumerical password. From the experiment it can be shown that none of users graphical password can be cracked, meanwhile 80% of the users' alphanumerical password can be cracked by the researcher. However in average, users need only 4.68 seconds to enter the password in alphanumerical password scheme, meanwhile in graphical password scheme it takes about 39.06 seconds. Hence password entry in the graphical password scheme needs about 8 times longer than in alphanumerical password. Based on this fact, the graphical password may still be considered to be used in applications that do not need a rapid password entry and the system security is becoming the main issue.

Keywords: graphical password, alphanumerical password, security.

INTRODUCTION

Nowadays, most systems that need user authentication will use alphanumerical password as their way to authentic the users. Despite its popularity, alphanumerical password has several drawbacks especially when it is used by novice users. Unaware of their lost if the password is known by others, these users usually choose their password to be short, easy to be guessed, or some other word related to their life such as their birthday, spouse or pets name, telephone number, and so on. This kind of password is categorized as a weak password and usually can be cracked easily by an unauthorized person.

In addition, it is not unusual to see some users writing down their password on a piece of paper, saving it in a mobile phone or other media, to assist them in recalling the password. This practice is definitely not recommended by all systems that need the users' password. However, without any assistance, these kinds of users may not be able to enter the systems since they can not recall the password. In a matter of fact, human ability in recalling is worse than the ability in recognition [1]. Remembering a person name is recalling, but remembering a person face is recognizing. That is why it is common for us to remember somebody face better than his/her name.

Moreover, most users are not involved with typing activity in their everyday life. Therefore these users usually type their password slowly, with just one or two forefingers. Consequently, unauthorized person can find the password easily by observing the movement of the users' fingers as they are entering the password. Finding somebody's password this way is called shoulder surfing.

A proposed solution to overcome this problem is to use a graphical password as a replacement to the alphanumerical password. A graphical password is a user authentication system where one or several pictures are used as a user's password. Instead of entering alphanumeric as a password, user has to select part or whole picture(s) as his/her password. Since human can perform recognition better than recalling, it is expected that the user will less forget his/her password.

This research will try to find the possibility of the replacement of alphanumerical password to a new graphical password scheme. Three parameters will be used to decide whether the replacement can be made or not. The three parameters are:

- easy to use: how many users can enter the password correctly
- speed: how long it takes for the users to enter the password
- security: how many passwords can not be stolen from the shoulder surfing activity

GRAPHICAL PASSWORD

Graphical password was introduced by Greg E. Blunder in 1996 [2]. In his scenario, the users have to select some points on the image as their password. The order and the position of the chosen points would become the users' password. In order to get access to the system, the users have to select the same positions of the image in the correct order. Unfortunately, the

requirement for the users to select the same and almost exact positions of the image in the correct order, raise difficulty for the users in entering their password. In addition, the display of the mouse cursor on the screen will make this scheme even easier to be cracked through shoulder surfing.

Dhamija and Perrig [3] proposing another kind of graphical password that they called Deja Vu. Instead of selecting several positions on the image, Deja Vu displayed several random images that should be selected by the users as their password. Since the size of the images are much larger than the size of the correct position allowed in the Blunder scheme, Deja Vu clearly has eliminated the problem of mistakenly select the image position when entering the password. The other good thing from Deja Vu is the usage of the abstract images provided to be selected as the users' password. Abstract images will make the password more secure than the ordinary image. In ordinary image, unauthorized person can guess users' password based on the users' preference. In spite of its advantage, the usage of abstract images raises a new problem to the users. Instead of recognizing, abstract images will force users to recall their password. Therefore users can forget their password easier than the one proposed by Blunder. Since in Deja Vu scheme, the users still have to direct the mouse pointer to the picture password, this scheme still easy to be cracked through shoulder surfing.

Figure 1. Several Pictures Displayed in PassFace Scheme

To overcome the problem of recalling the picture, Davis et al [4] proposing a graphical password that he called PassFace. Instead of selecting random images, Davis displays several images of human faces that should be selected by the users as their password (see figure 1). For this purpose, Davis provides several hundreds images of human faces to be selected by the users. The advantage of this password scheme is the high ability of the users to recognize their password. This is due to the high ability of human to perform recognition instead of recalling. Unfortunately, this password scheme is still easy to be cracked through shoulder surfing. In addition the users tendency to choose faces that have the same ethnic or gender as they are, make the password even easier to be guessed based on the users' identity or preference.

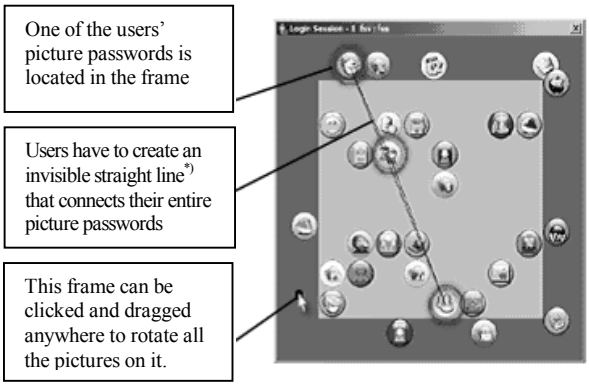
MOVABLE FRAME GRAPHICAL PASSWORD

One characteristic of the previous graphical passwords that make them easy to be cracked through shoulder surfing is the requirement to select the pictures that becoming the password [5]. Since the movement of the mouse cursor on the screen can be spotted easier than the key pressed on the keyboard, all previous graphical password schemes can be cracked easier than the alphanumerical password. Therefore it is necessary to find a graphical password scheme that does not obligate the users to select their picture password when they are entering the password.

One possible solution is to let users arrange their picture passwords to build an invisible simple mathematical object such as line, triangle, etc. This arrangement must be able to be carried out with or without pointing out to the users' picture passwords. One proposed scenario is to disperse a number of pictures on a certain box and put three users' picture password on it. This box is separated into two parts, the outer part and the inner side. One of users' picture passwords is placed in the outer part of the box, and the other two are placed in the inner part. The users have to create an invisible straight line composed from their three picture passwords as a means to enter the password (see figure 2). To create the invisible straight line, the users can rotate the outer part or the frame of the box by clicking and dragging the mouse cursor in any part of the frame. Since the users are not necessarily put the mouse cursor on their picture password, this password scheme is expected to be more secure from the shoulder surfing attacker than the other password scheme.

Although this password scheme looks hard enough to be cracked through shoulder surfing, it still has to be protected from an unauthorized person that tries to guess the password by randomly move the frame. If the other password schemes need only one valid input, this scheme may need several valid inputs to enter the system. In this research, the users have to provide three valid inputs as a valid password.

Between each input, all pictures will be scattered again in random positions. Therefore the possibility of an unauthorized person to get the valid password by randomly moving the frame can be said almost impossible.



*) Note: the line that connected the users' picture passwords is shown for explanation only

Figure 2. Moveable Frame Graphical Password

REQUIREMENT

In order to get the users input, the moveable frame picture password must be implemented first. The application is created using Visual Basic and will be run on Pentium 4 computer with Windows operating system. Some analyses that serve as a basis for the implementation of the picture password software are:

- The position for each picture should not be placed in completely random position. Placing the pictures in completely random positions will make some pictures overlap to each other and can not be seen clearly. Therefore the pictures will be placed in a kind of invisible grid that guarantee no overlap will occur. Each location in the grid is called cell.
- The size of the cell does not have to be the same with the size of the picture. However the cell size must be larger than the picture size to guarantee no overlap will occur, and to provide distance between each picture. The distance between each picture will ease the users in finding the picture passwords
- The new position of all pictures in the second or third entries should not be changed abruptly. However, these pictures should be moved (animated) to a new position with a certain speed. Therefore users can follow the movement of their picture password to a new position and do not have to search their picture password again. It is expected that the time required by the users to find their picture password in the second and third entries will be less than the first entry.
- There should be a tolerance to the invisible straight line created by the users. This tolerance should not be too small or too big. A very small tolerance will force the users to create an almost exact straight line as a valid entry, meanwhile a very big tolerance will make invalid entry will be accepted as a valid one.
- The system should give tolerance time for the users to change their entry as they release the mouse button. The time is provided for the users to reconstruct the invisible straight line if they think the line is not straight enough. However the system should allow them to skip this tolerance time as well. Therefore confident users can go through the next entries without having to wait this tolerance time.

METHODOLOGY

In this research, 10 respondents will be asked to enter the alphanumeric password and the graphical password. All respondents are 18 years old or above with at least high school educational background. Although all the respondents have ever been using computer for some purpose but they are not using it in their everyday life. Therefore they were expected as a representation of the novice users who can not type fast enough to hide their password from the shoulder surfing attacker.

In order to prove the weakness of each password scheme from the shoulder surfing attacker, the researcher will try to steal the password from all respondents as they entering theirs. The main objectives of this experiment are to discover the easiness, speed and security of each password scheme. The easiness of the password can be measured by the number of correct passwords that are entered by the user. Meanwhile the security of the password is measured by the number of passwords that can not be stolen by the researcher.

Before the experiment began, all the respondents were gathered to get the explanation about the purpose of the experiment. In addition, they were informed that the researcher will try to steal their passwords as they entering theirs. The researcher guarantees that the stolen password will be kept secret and will not be published. In order to standardize the experiment the users have to choose and enter the password based on these criteria:

- Alphanumerical Password:
  - ❑ the password can be composed from any characters available on the keyboard
  - ❑ the length of the password must be longer than 6 characters

- ❑ respondents should type their password using one or two finger(s) only
- ❑ if the respondents can not remember their password, they have to enter any characters that they think was the password

- Movable frame graphical password
  - ❑ the password must be chosen from more than three pictures although only three pictures will be shown on the box at a time
  - ❑ each pictures selected must be unique
  - ❑ to validate a password, the respondents should create a valid straight line thrice

To find out the easiness in remembering the password, the experiment is scheduled for several days. On the first day, the respondents will be trained about inputting the password in the alphanumerical and movable frame graphical password. After the training, they were asked to enter their password thrice. Since movable frame graphical password needs three valid inputs as a valid password, therefore the number of inputs that should be performed by each user in the graphical password is nine. The time interval between each process is 15 minutes. On the next six days, the respondents have to enter their password daily, once for each day. Two weeks after the first experiment day, they were asked to enter their password once again for the last time. Therefore, each respondent will carry out 10 experiments for each scheme.

Meanwhile, the characteristics of the system used as an instrument for the users to enter the password are:

- General:
  - ❑ All schemes will have a user name and password section. The users should enter the user name first before entering the password.
  - ❑ The time required for the respondents to enter the password will be counted as soon as the respondents move from the user name to the password section.
- Alphanumerical password:
  - ❑ All characters entered by the users as a password will be displayed as points.
  - ❑ Users can enter their password once.
- Movable frame graphical password
  - ❑ The grid size of the cell is 10 x 10
  - ❑ The numbers of pictures available are 400. However only 75 pictures will be shown on the box at a time. 50 pictures will be displayed inside the box, and 25 pictures on its frame. All pictures are colored.
  - ❑ The maximum distance between each password picture is 5 cells and the minimum distance is 2 cells
  - ❑ The error tolerance for the straight line is 20 pixels
  - ❑ The time tolerance before the arrangement of the pictures is accepted as an input is 10 seconds

RESULT

For a new user, the moveable frame graphical password application provides a collection of pictures that can be chosen as the password (see figure 3). The researcher tried to provide as general pictures as possible. By providing the general picture, the users can not choose the picture passwords that belong to their preferences. Therefore, guessing the users password will be more difficult to be done. Some of the picture categories that can be considered as the users' preferences and should be avoided are the picture of human face, animal, plant, electronic stuff, etc. The pictures provided in this application are taken from the operating system Windows and some other Windows application icon.

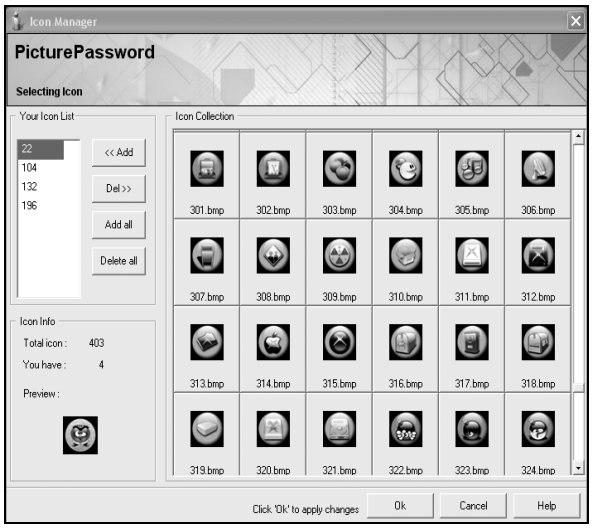


Figure 3. Selecting The Picture as a Password

Users that have already had a picture password can continue the process by entering their picture password. Figure 4 shows a state where a user is in the process of entering the password. The border of the box will be colored dark grey as the user moving the moveable frame, and will gradually turn to white as the mouse button is released. As stated in the scenario above, the users have to enter correctly their picture password thrice before the system considers it as a valid password.

Figure 4. Entering The Password

Meanwhile, the complete result of the experiments can be seen in table 1 and 2. Surprisingly enough, although the alphanumerical password was commonly used and most people have experienced it at least once in their life, some users fail to enter the password correctly. This failure is coming from the obligation for the users to build their password using more than 6 characters. Therefore some users can not choose their commonly used password and forget it in several days later. Total entries in the alphanumerical password are 100 and the incorrect entries are 17. The reasons behind these failures are:

1. The users can not recall their password (5 entries)
2. The users mistakenly typed their password (12 entries)

Meanwhile, in the moveable frame graphical password, the failure of entries in this password scheme is 31. Total entries in the moveable frame graphical password are 100. The reasons behind these failures are:

1. The users can not recognize some of their picture passwords (9 entries). As instructed, all users have more than three pictures as their password. However, only three picture passwords will be shown at a time. One or several pictures that seldom appear will make the users forget the password.
2. The users mistakenly choose their picture password (1 entry). In the experiment the researcher had tried to provide 400 different pictures. However, some pictures may still look similar to each other. Therefore, when these pictures appear together with the users' picture password, some users choose the incorrect picture as their password.
3. The line built by the three picture passwords is not straight enough (21 entries). Creating an invisible straight line may not be easy for some users. Therefore some users' incorrect input originated from the unacceptable straight line. This is the major reason of the incorrect entries.

Table 1. The Experiment in Entering The Movable Frame Graphical Password

U	E_1		E_2		E_3		E_4		E_5		E_6		E_7		E_8		E_9		E_{10}		S/F		Avg	min	max
	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	S	F			
1	S	34.3	F	34.12	F	30.12	F	32.1	S	37.77	S	40.12	S	35.1	S	43.33	S	31.25	F	40.23	6	4	36.978	31.25	43.33
2	S	40.23	S	44.2	S	41.19	F	38.7	F	36.45	S	33.15	S	28.4	S	26.47	S	43.4	S	36.66	8	2	36.713	26.47	44.2
3	S	54.5	S	44.4	S	43.1	S	32.12	S	44.54	S	34.4	S	38.8	S	35.06	S	41.4	S	43.44	10	0	41.176	32.12	54.5
4	S	49.5	S	50.51	S	44.66	F	27.5	F	10.5	F	23.2	F	14.51	F	17.2	F	11.52	F	10.05	3	7	48.223	44.66	50.51
5	S	32.22	S	39.45	S	40.12	S	42.2	S	40.15	S	29.5	S	37.7	S	40.5	S	39.99	S	40.05	10	0	38.188	29.5	42.2
6	F	40.05	F	22.15	F	25.46	F	15.5	F	20.5	F	30.64	F	29.8	F	22.25	F	14.4	F	30.61	0	10	0	-	-
7	S	32.5	F	35.5	S	39.4	S	34.88	F	40.1	S	38.71	F	31.16	S	34.46	S	29.7	F	34.46	6	4	34.942	29.7	39.4
8	S	37.7	S	44.12	S	43.21	S	37.5	S	36.5	S	40.12	S	45.4	S	44.17	S	38.6	F	47.77	9	1	40.813	36.5	45.4
9	S	47.15	S	38.86	S	41.56	S	36.6	S	39.9	S	26.55	F	32.56	S	45.6	F	49.2	F	42.5	7	3	39.46	26.55	47.15
10	S	34.2	S	27.6	S	25.4	S	28.8	S	30.1	S	36	S	38.07	S	40.4	S	44.29	S	45.73	10	0	35.059	25.4	45.73
																				Total	**69**	**31**			

Description:
U : user number
E_n : the n^{th} experiment
R : the result of the experiment. S for success and F for fail.
T : the duration of time (in second) required to enter the password
S/F : the number of success and failure
Avg : average time for the success entries
min : the fastest time recorded in entering the password
max : the slowest time recorded in entering the password

Table 2. The Experiment in Entering The Alphanumerical Password

U	E_1		E_2		E_3		E_4		E_5		E_6		E_7		E_8		E_9		E_{10}		S/F		Avg	min	max
	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	R	T	S	F			
1	S	5.2	S	4.81	S	4.66	S	4.81	S	5.45	S	4.88	S	4.9	S	5.12	S	5.77	S	5.6	10	0	5.12	4.66	5.77
2	S	6.1	S	6.31	S	6.27	S	5.94	S	6.03	S	6.4	S	6.35	S	6.37	S	5.78	S	6.12	10	0	6.167	5.78	6.4
3	S	3.11	S	2.3	S	2.19	S	2.1	S	2.24	S	2.14	S	2.22	S	2.41	S	2.06	S	2.33	10	0	2.31	2.06	3.11
4	S	4.08	F	4.66	S	4.81	S	4.12	S	3.9	S	4.31	S	4.07	S	4.16	S	4.12	S	3.55	9	1	4.1244	3.55	4.81
5	S	6.9	S	7.15	S	7.23	S	7.41	S	6.46	F	6.56	S	7.05	S	6.7	S	6.23	F	7.9	8	2	6.8913	6.23	7.41
6	S	5.15	S	4.75	S	5.23	S	9.23	F	12.5	F	20.6	F	6.35	F	6.11	F	4.03	F	5.09	4	6	6.09	4.75	9.23
7	S	5.2	S	4.98	S	4.86	S	5.36	S	4.92	S	4.72	S	5	S	4.8	S	5.12	F	4.06	9	1	4.9956	4.72	5.36
8	S	3.08	S	3.41	S	2.7	S	2.72	S	2.9	S	2.6	S	3.16	S	2.78	S	4.12	S	3.66	10	0	3.113	2.6	4.12
9	S	1.41	S	1.44	S	1.39	S	1.45	S	1.5	S	2.01	S	1.39	S	1.6	S	1.43	S	2.2	10	0	1.582	1.39	2.2
10	S	6.25	S	6.3	S	6.7	F	6.66	F	8.1	F	7.5	F	5.5	F	5.1	F	5.36	F	5.88	3	7	6.4167	6.25	6.7
																				Total	**83**	**17**			

Description:
U : user number
E_n : the n^{th} experiment
R : the result of the experiment. S for success and F for fail.
T : the duration of time (in second) required to enter the password
S/F : the number of success and failure
Avg : average time for the success entries
min : the fastest time recorded in entering the password
max : the slowest time recorded in entering the password

The average time required for the success entries in the alphanumerical password is 4.68 seconds, while in movable frame graphical password is 39.06 seconds. Therefore in average, the time required to enter the password in the movable frame graphical password is 8 times longer than in alphanumerical password. Inputting the password in the movable frame graphical password is expected will need longer time than in alphanumerical password since a lot of activities are required in entering the password. Firstly the users have to search the picture password. Secondly, they have to rotate the frame and predict that all of their picture passwords have been in a straight line; and finally, all of those activities must be performed thrice.

However, the average entries time for the moveable frame graphical password is considered longer than the initial researcher expectation. It is expected that the movable frame graphical password will need four or five time longer than the alphanumerical password. The reason behind this expectation is coming from the fact that the users have to enter three valid inputs as one valid password. In addition, before the inputs can be performed, the users have to search their picture password first. Unfortunately, this research proves that in the average, users need eight times longer to input password in moveable frame graphical password. One good thing that should be noted is that the fastest time required to enter the moveable frame graphical password is 25.4 seconds. This recorded time is just about 3 times longer than the slowest time required in entering the alphanumerical password. Therefore, there is still a possibility to improve the average time required to enter the moveable frame graphical password.

As informed to the users, the researcher will try to cracked their password through shoulder surfing. Table 3 shows the result of this activity. From table 3, it can be seen that almost all (80%) alphanumerical password can be cracked through shoulder surfing when the users type the password with just one or two fingers only. Meanwhile, none of the moveable frame graphical password can be cracked by the researcher. Even though none of the moveable frame graphical password can be cracked by the researcher, two picture passwords from user number 5 and 10 can be found out. Having two of three pictures password still can not guarantee the unauthorized person to enter the system. This is because the third picture password can not be guessed from the two pictures found. In contrast the unauthorized person can guess easily one or several missing characters in the alphanumerical password when they have found the key characters of the password. This is because most users usually create a patterned alphanumerical password.

Table 3. Shoulder surfing result

User	Alphanumeric	Moveable frame
1	Cracked	Can not be cracked
2	Cracked	Can not be cracked
3	Cracked	Can not be cracked
4	Cracked	Can not be cracked
5	Cracked	Only 2 pictures found
6	Cracked	Can not be cracked
7	Can not be cracked	Can not be cracked
8	Cracked	Can not be cracked
9	Can not be cracked	Can not be cracked
10	Cracked	Only 2 pictures found

CONCLUSION

From the experiments it can be concluded that the moveable frame graphical password is really secure. It can be said that this password scheme is almost impossible to be cracked through shoulder surfing. Therefore this password scheme is suitable for application that needs high security, such as the network administrator or credit card authentication etc.

Despite its advantage, the moveable frame graphical password has several drawbacks that should be overcome in the next research. One major drawback of the moveable frame graphical password resides on the length of the time required to enter the password. To avoid unauthorized person cracking the password by performing some guesses, the moveable frame graphical password requires three correct inputs as a valid password. If one of the inputs is incorrect, the users are still not allowed to enter the system, although two other inputs are correct. Future research can be performed to find out the possibility of decreasing the number of iteration needed to validate the password. The future research can also be performed in finding the pictures that are completely different from one another. These completely different pictures are predicted can decrease the length of time required by users in finding their picture password.

In conclusion, until the recent state, the movable frame graphical password can only be used in an application that needs better security but does not need a rapid time for the password entry. The replacement of the alphanumerical password to the moveable frame graphical password for the public machine – where most users access it in a very short time – is not recommended yet.

REFERENCES

1. Gatech. Human Memory. http://www.cc.gatech.edu/classes/cs6751_97_winter/Topics/human-cap/memory.html. 1997.
2. Greg E Blunder. *Graphical Password*. United Stated Patent 5559961. 1996
3. Dhamija, R.; Perrig, A. *Deja Vu*: *A User Study Using Images For Authentication*. Ninth Usenix Security Symposium. 2000.
4. Davis, D.; Monrose, F.; Reiter, M.K. *On User Choice in Graphical Password Schemes*. Procceedings of the 13th USENIX Security Symposium. San Diego. 2004.
5. Sobrado, L; Briget, J.C. Graphical Passwords. New Jersey, USA. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm. 2002.